(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 July 2001 (12.07.2001)

PCT

(10) International Publication Number
WO 01/50429 A1

(51) International Patent Classification[7]: G07F 19/00

(21) International Application Number: PCT/US01/00400

(22) International Filing Date: 4 January 2001 (04.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/174,564 5 January 2000 (05.01.2000) US

(71) Applicant: **AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC.** [US/US]; American Express Tower, World Financial Center, New York City, NY 10285-4900 (US).

(72) Inventors: **GRAY, William, J.**; Apartment C-513, 350 South 200 West, Salt Lake City, UT 84101 (US). **HOHLE, William**; 10882 West Cedar Fort Road, 8570 North, Lehi, UT 84043 (US). **LARKIN, Carl**; Vine Cottage, Yapton Road, Barnham, Bognor Regis, West Sussex PO22 0AY (GB). **PEART, Lee, J.**; 48 Cedar Drive, Southwater, West Sussex FH1 7UF (GB).

(74) Agent: **SOBELMAN, Howard, I.**; Snell & Wilmer L.L.P., One Arizona Center, 400 E. Van Buren, Phoenix, AZ 85004-2202 (US).

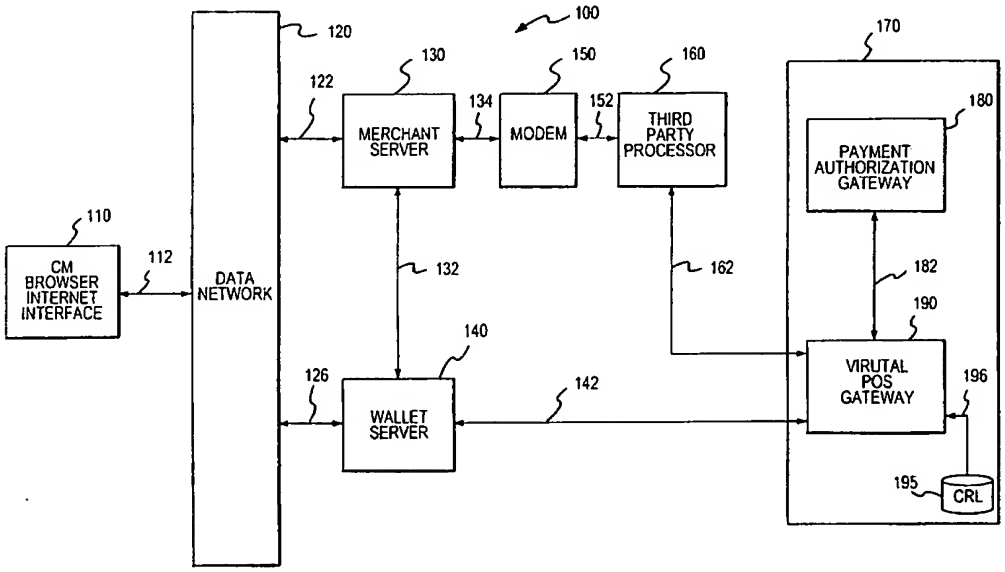
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

[Continued on next page]

(54) **Title:** SMARTCARD INTERNET AUTHORIZATION SYSTEM



(57) **Abstract:** A system and method are disclosed for conducting electronic commerce such as a virtual purchase transaction with an on-line merchant. A user is provided with an intelligent token, such as a smart card containing a digital certificate. The intelligent token suitably authenticates with a wallet server on a network that conducts all or portions of the transaction on behalf of the user without requiring changes to the merchant's server. The wallet server interacts with a security server of a selected financial service to provide authentication of the transaction. Upon authentication, the digital wallet prefills forms which are transmitted to the merchant who contacts the security server for validation of the forms and upon validation, completes the transaction with the user.

WO 01/50429 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SMARTCARD INTERNET AUTHORIZATION SYSTEM

FIELD OF THE INVENTION

The invention relates generally to methods and apparatus for conducting network transactions, and more particularly, to systems for authenticating and conducting business over data networks such as the Internet.

BACKGROUND OF THE INVENTION

In recent years, many consumers have discovered the convenience and economy of purchasing goods and services electronically. A number of channels for electronic purchases (commonly called "e-purchases") are available, including shop-at-home television networks, call-in responses to television advertisements, and the like. Most recently, direct purchasing via the Internet has become extremely popular.

In a typical Internet transaction, a consumer generally identifies goods and/or services for purchase by viewing an online advertisement such as a hypertext markup language (HTML) document provided via a World Wide Web (WWW) browser. Payment typically occurs in various ways. One such way is via a charge card number that is provided via a secure channel such as a secure sockets layer (SSL) connection that is established between the consumer and the merchant.

While millions of such transactions take place every day via the Internet, these conventional SSL transactions often exhibit a number of marked disadvantages. Although SSL typically provides a secure end-to-end connection that prevents unscrupulous third parties from eavesdropping (e.g., "sniffing") or otherwise obtaining a purchaser's charge card number, the protocol does not provide any means for ensuring that the charge card number itself is valid, or that the person providing the card number is legally authorized to do so. Because of the high incidence of fraud in Internet transactions, most charge card issuers consider network transactions to be "Card Not Present" transactions subject to a higher discount rate. Stated another way, because of the increased risk from "Card Not Present"

transactions, most charge card issuers charge the merchant a higher rate for accepting card numbers via electronic means than would be charged if the card were physically presented to the merchant.

To improve the security deficiencies inherent in transporting charge card numbers over unsecure networks, many have suggested the use of "smart cards". Smartcards typically include an integrated circuit chip having a microprocessor and memory for storing data directly on the card. The data can correspond to a cryptographic key, for example, or to an electronic purse that maintains an electronic value of currency. Many smart card schemes have been suggested in the prior art, but these typically exhibit a marked disadvantage in that they are non-standard and typically require the merchants to obtain new, proprietary software for their Web storefronts to accept the smart card transactions. Moreover, the administration costs involved with assigning and maintaining the cryptographic information associated with smart cards have been excessive to date.

Another standard, the Secure Electronic Transaction (SET) standard has been suggested to improve the security of Internet transactions through the use of various cryptographic techniques. Although SET does provide improved security over standard SSL transactions, the administration involved with the various public and private keys required to conduct transactions has limited SET's widespread acceptance. SET also requires special software for those merchants wishing to support SET transactions.

Additionally, existing digital wallet technology, such as the digital wallet technology provided by, for example, GlobeSet, Inc., 1250 Capital of Texas Highway South, Building One, Suite 300, Austin, TX, 78746, is being more frequently used to provide a means for users to utilize transaction card products (e.g., credit, charge, debit, smart cards, account numbers and the like) to pay for products and services on-line. In general, digital wallets are tools which store personal information (name, address, chargecard number, credit card number, etc.) in order to facilitate electronic commerce or other network interactions. The personal information can be stored on a general server or at a client location (PC or Smartcard) or on a hybrid of both a general server and a client server. Presently, the digital wallet general server is comprised of a Web server and a database server which centrally houses

the user's personal and credit card information, shopping preferences and profiles of on-line merchants.

A digital wallet preferably performs functions such as single sign on/one password, automatic form filling of check out pages, one or two click purchasing, personalization of Websites, on-line order and delivery tracking, itemized electronic receipts, and customized offers and promotions based upon spending patterns and opt-ins. More particularly, a one-click purchase activates the wallet and confirms the purchase at the same time. A two-click check out first activates the wallet, then the second click confirms the purchase. In use, the wallet bookmark is typically clicked by the user and an SSL session is established with the Wallet server. A browser plug-in is executed and the user supplies an ID/password or smart card for authentication in order to gain access to the wallet data. When shopping at an on-line merchant, the appropriate wallet data is transferred from the wallet server to the merchant's Web server.

Existing systems, however, generally require that a merchant initiate changes to accommodate each different smart card or wallet. Accordingly, a new system of conducting electronic transactions is desired which would provide improved security with minimal overhead for users and merchants. Moreover, such a new system should integrate well with various smart cards and Internet wallets and other services provided by various merchants without requiring the merchant to make substantial changes to permit use of different systems.

SUMMARY OF THE INVENTION

In an exemplary embodiment of the invention, a user is provided with a smart card having a standardized protocol to make credit and debit transactions, such as, for example, the Blue™ from American Express™ smart card or the Europay MasterCard™ Visa™ (EMV) smart card. The user, also known as the cardmember (CM), utilizes the EMV Smartcard to interface with a wallet server to authenticate the user with a merchant server on a network through communications with a security server provided by a financial institution or credit provider such as, for example, American Express (AMEX). The CM purchaser conducts a virtual purchase transaction via the internet

through a wallet server interacting with the security server to provide enhanced reliability and confidence in the transaction.

The user logs onto the internet via a browser and selects a wallet, causing the establishment of a secure sockets layer link to the wallet server and, at about the same time, activates the client window. The wallet server requests the user to insert the smartcard for authentication to the server wallet account. With an encrypted identity certificate being set, the user then selects the credit provider/financial institution, such as AMEX, who will be providing guarantee of the payment, from the provider available in the wallet. The user then logs onto the merchant server, completes shopping, goes to the checkout screen and clicks secure checkout. Again, the interfaces are over a secure sockets layer.

Next, the wallet server completes the form and transmits it to the merchant server, which uses telephone connections via a modem, direct link to a third party processor or directly to the security processor of the credit provider. The credit provider security processor uses the wallet interface to the user card to access smartcard functionality and generates a signed transaction. Alternatively, the connection can also be used to securely update functionality as required. The AMEX security processor authorizes the transaction on a "card press" basis. The merchant server then integrates the authorization with the wallet server completed form received from the wallet server and successfully completes the transaction, informing the user that the transaction has been successfully completed.

Thus, electronic transactions, such as purchase transactions, are conducted by receiving a transaction request from a user at a wallet server, issuing a challenge to the user from the wallet server, receiving a response from the user based upon the challenge, processing the response to verify the transaction instrument, assembling credentials (including authorization for the electronic transaction), and interfacing with a security server to authenticate the transaction. The system provides the benefits of protecting the market and the credit provider from fraud, transaction non-imputation, an ability to modify parameters on-line, and providing the user with better service at a lower cost by reducing the costs to the merchant because the entire process is transparent to the merchant.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other features and advantages of the present invention are hereinafter described in the following detailed description of exemplary embodiments to be read in conjunction with the accompanying drawing figures, wherein like reference numerals are used to identify the same or similar parts or steps in the similar views, and:

Figure 1 is a block diagram of an exemplary embodiment of the transaction system of the present invention; and

Figure 2 is a diagram of an exemplary process executed by the exemplary transaction system of Figure 1.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

The present invention may be described herein in terms of functional block components and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the present invention may employ various integrated circuit (I.C.) components, e.g., memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, or the like, with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. Still further, the invention could be used to detect or prevent security issues with a scripting language, such as JavaScript, VBScript or the like. For a basic introduction of cryptography, please review a text written by Bruce Schneider which is entitled "Applied Cryptography: Protocols, Algorithms, And Source Code In C," published by John Wiley & Sons (second edition, 1996), which is hereby incorporated by reference.

It should be appreciated that the particular implementations shown and described herein are illustrative of the invention and its best mode and are not intended to otherwise limit the scope of the present invention in any way. Indeed, for the sake of brevity, conventional data networking, application development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical electronic transaction system.

To simplify the description of the exemplary embodiment , the invention is described as pertaining to a system of electronic commerce, i.e., transactions, running over the Internet. It will be appreciated, however, that many applications of the present invention could be formulated. For example, the system could be used to authenticate users of a computer system, or to activate a passcode system, or any other purpose. One skilled in the art will appreciate that the network may include any system for exchanging data or transacting business, such as the Internet, an intranet, an extranet, WAN, LAN, satellite communications, and/or the like. Communication between the parties to the transaction and the system of the present invention is accomplished through any suitable communication means, such as, for example, a telephone network, Intranet, Internet, point of interaction device (point of sale device, personal digital assistant, cellular phone, kiosk, etc.), online communications, off-line communications, wireless communications, and/or the like. The users may interact with the system via any input device such as a keyboard, mouse, kiosk, personal digital assistant, handheld computer (e.g., Palm Pilot®), cellular phone and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, workstation, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, or the like. Moreover, although the invention is frequently described herein as being implemented with TCP/IP communications protocols, it will be

readily understood that the invention could also be implemented using IPX, Appletalk, IP-6, NetBIOS, OSI or any number of existing or future protocols.

Furthermore, the user and merchant may represent individual people, entities, or business and while reference is made to AMEX, this is by way of example and the financial authorization entity may represent various types of card issuing institutions, such as banks, credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. The payment network includes existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards.

Additionally, other participants may be involved in some phases of the transaction, such as an intermediary settlement institution, but these participants are not shown. Each participant is equipped with a computing system to facilitate transactions. The user has a personal computer, the merchant has a computer/server, and the financial authorization entity has a main frame computer; however, any of the computers may be a mini-computer, a PC server, a network set of computers, laptops, notebooks, hand held computers, set-top boxes, and the like.

The customer and merchant may represent individual people, entities, or business. Although labeled as a "bank," the bank may represent other types of card issuing institutions, such as credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. It is further noted that other participants may be involved in some phases of the transaction, such as an intermediary settlement institution, but these participants are not shown.

Each participant is equipped with a computing system to facilitate online commerce transactions. The customer has a computing unit in the form of a personal computer, although other types of computing units may be used including laptops, notebooks, hand held computers, set-top boxes, and the like. The merchant has a computing unit implemented in the form of a computer-server, although other implementations are possible. The bank has a computing center shown as a main frame computer. However, the bank computing center may be implemented in other forms, such as a mini-computer, a PC server, a network set of computers, and the like.

The computing units are connected with each other via a data communication network. The network is a public network and assumed to be insecure and open to eavesdroppers. In the illustrated implementation, the network is embodied as the internet. In this context, the computers may or may not be connected to the internet at all times. For instance, the customer computer may employ a modem to occasionally connect to the internet, whereas the bank computing center might maintain a permanent connection to the internet. It is noted that the network may be implemented as other types of networks, such as an interactive television (ITV) network.

The merchant computer and the bank computer are interconnected via a second network, referred to as a payment network. The payment network represents existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards. The payment network is a closed network that is assumed to be secure from eavesdroppers. Examples of the payment network include the American Express®, VisaNet® and the Veriphone® network.

The electronic commerce system is implemented at the customer and issuing bank. In an exemplary implementation, the electronic commerce system is implemented as computer software modules loaded onto the customer computer and the banking computing center. The merchant computer does not require any additional software to participate in the online commerce transactions supported by the online commerce system.

A customer account number may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". The first five to seven digits are reserved for processing purposes and identify the issuing bank, card type and etc. In this example, the last sixteenth digit is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer.

Referring now to **Figure 1**, a transaction system 100 typically includes at least one user or cardmember (CM) having a computer incorporating an

internet browser 110 adapted to interface with a data network. In an exemplary embodiment, transaction system 100 is used in electronic commerce to conduct purchase transactions. It will be appreciated that although the transaction system described herein is an electronic commerce system, the present invention is equally applicable to various other electronic transaction systems. Specifically, the user system 110 is a purchaser or user which interfaces with a computer having an interface through data network 120 to a merchant server 130 and also to a digital wallet server 140.

The various computer systems and servers are interconnected as appropriate by data network 120, which is any data network, such as the internet or other public or private data network. Other suitable networks 120 include the public switch telephone network (PSTN), wireless networks, corporate or university intranets, and the like. Additionally, merchant server 130 is coupled to a modem 150 which is in communication with a third party processor (TPP) 160 which may be, but is not necessarily included, in the financial authorization entity secure processor 170. TPP 160 is further coupled to a virtual point of sale (POS) gateway processor 190 which is in the financial authorization entity secure processor 170. Also in the secure processor 170, and coupled to POS gateway processor 190, is payment authorization gateway 180. Further, wallet server 140 is coupled to merchant server 130 and to virtual point of sale (VPOS) gateway processor 190.

While an exemplary embodiment has been illustrated in **Figure 1**, it will be appreciated that other embodiments are possible. Thus, as also described above, components (e.g., user 110, merchant 120, and wallet server 140) may be individual computers or network groups of computers acting with similar purpose to fulfill the functions described herein. Functionality attributed to a single component may be distributed among one or more individual computers in order to fulfill the described functionality. For example, the wallet server 140 may in fact be a collection of web servers, application servers, data base servers, and other types of servers. Also, in various embodiments, data bases (not shown) and/or profile servers (not shown) may be connected to wallet server 140. For further information related to smart cards, browser functions, digital wallets and e-commerce transactions, see U.S. patent applications "Transaction Card", U.S. Serial No.

9/653,837, filed on September 1, 2000; "Method and Apparatus for Conducting Electronic Transactions", U.S. Serial No.: 09/652,899, filed on August 31, 2000; "System and Method For Authenticating A Web Page", U.S. Serial No. 09/656,074, filed on September 6, 2000; and, "System and Method For Profiling A Web Site", U.S. Serial No. 09/656,061, filed on September 6, 2000, all of which are herein incorporated by reference.

To conduct a transaction, user 110 suitably establishes a connection through network 120 with a merchant 130. When a purchase is to be consummated, user 110 accesses wallet server 140. User 110 is then directed by wallet server 140 to insert a Smart Card into the system to verify that a Smart Card is in the user's 110 possession. At the same time, a graphical representation of wallet 140 appears to the user 110 and user 110 is directed to select a transaction authorization entity, such as American Express (AMEX). The Smart Card preferably includes a digital certificate that uniquely identifies the card such that digital credentials relating to the transaction may be created as described hereinafter. Upon receipt of the Smart Card information, wallet server 140 communicates with virtual POS gateway 190.. Virtual gateway 190 queries payment authorization gateway 180 to obtain authorization for the payment. Upon obtaining such authorization, virtual POS gateway transmits the information to wallet server 140. Wallet server 140 then completes an authorization form and transmits the form to merchant server 130.

Upon receipt of the authorization form, merchant server via modem 150 communicates with third party processor 160, which in turn communicates with virtual POS gateway 190, again querying payment authorization gateway 180. Again, virtual POS gateway 190 communicates through third party processor 160 via modem 150 to merchant server 130, authenticating the completed form. Once completed, merchant server 130 authorizes the transaction and the transaction is completed, and the user 110 is notified.

Referring also to **Figure 2**, the flowchart shows an exemplary sequence of events involved in the on-line virtual transaction. As shown at step (210), a virtual transaction purchase by a customer is begun on-line, with a customer communicating with a vendor. At the completion of shopping, the

customer or user 110 initiates a secure checkout procedure as shown in step (220), opening the wallet and interfacing a Smart Card with the wallet server 140, including selecting the credit supplier. The wallet server 140 interfaces at step (220) with a security server to authenticate the transaction. In step (240), the wallet server 140 receives transactional authentication, completes an authorization form for the transaction and transmits the form to the merchant server 130. In step (250), the merchant server queries the security server for credit supplier authentication of the authorization form. Based on the information supplied by the credit supplier, and in conjunction with the authentication above discussed in the previous steps, the credit supplier authenticates the authorization form based on the information from the Smart Card provided through the wallet server and transmits an authentication to the merchant server 130. Upon receipt of the authorization form, the merchant completes the virtual transaction/purchase, informing the customer and debiting the customer's account.

Because the Smart Card as above-described contains identifying information that is unique to a particular card, the purchase transaction conducted with the Smart Card is more secure than a transaction conducted with an ordinary charge or credit card. Accordingly, a discount rate may be justified for the secure transaction, which may be processed by the card issuer as a "card present" transaction. Additionally, if the transaction is a "card present" transaction, risk of fraud may be transferred from the merchant to the card issuer.

Thus, the present invention is directed to a system and method for permitting the authentication of a virtual on-line transaction where a user, by the use of a Smart Card and a wallet server, may have on-line virtual transactions authenticated to a merchant using various Smart Cards and credit providers while minimizing changes to the merchant's server to accommodate a number of different types of systems.

Accordingly, corresponding structures, acts, and equivalents of all elements in the claims below are intended to include any structural material or acts for performing the functions in combination with other elements as specifically claimed. The scope of the invention should be determined by the

allowed claims and their legal equivalents, rather than by the examples given above.

CLAIMS

What is claimed is:

1. A method for conducting a transaction, the method comprising:

a. receiving a request to authenticate a transaction from a user at a server;

b. requiring the user to provide an instrument for verification;

c. receiving an instrument input response from the user based upon said requirement;

d. processing said instrument input as an input to a security processor;

e. assembling forms for the transaction, said forms comprising said security processor authorization of said input to said security processor;

f. providing said forms incident to said transaction and sending a request to said security processor for a second authorization of said forms; and

g. validating said transaction with said second authorization of said forms received from said security processor.

2. The method of Claim 1 further directed to providing such transaction validation for different combinations of instruments and security processors without requiring changes to transaction processing by said merchant.

3. The method of Claim 1, wherein the transaction is an electronic purchase transaction.

4. The method of Claim 3, wherein the electronic purchase transaction is conducted using a digital wallet.

5. The method of Claim 1, wherein the instrument is a smart card.

6. A method for providing secure virtual transactions between a user and a an on-line merchant without requiring changes at the merchants location, the method comprising:

a. developing a first query for transmission to a credit provider;

b. receiving a response from said credit provider and transmitting same to said merchant;

c. said merchant querying said credit provider for authentication of said credit provider response; and

d. completing said virtual transaction using authorization from said credit provider.

7. The method of Claim 6 wherein said first query is developed by opening a wallet and inputting information from a smart card.

8. The method of Claim 6, further comprising developing a form from said response from said credit provider and transmitting said form to said merchant.

9. The method of Claim 8, wherein said merchant requests authentication of said form from said credit provider.

10. The method of Claim 6, wherein said credit provider is selected by said user from a group of credit providers.

11. The method of Claim 9, wherein said credit provider is selected by said user from a group of credit providers..

12. A method for conducting a transaction, the method comprising:

a. receiving a request to authenticate a transaction with a merchant from a server;

b. requiring an instrument for providing verification;

c. receiving an instrument input response based upon said requirement;

d. processing said instrument input as an input to a security processor;

e. assembling forms for the transaction, said forms comprising said security processor authorization of said input to said security processor;

f. providing said forms incident to said merchant;

g. said merchant processing said forms and sending a request to said security processor for a second authorization of said forms; and

h. validating said transaction with said second authorization of said forms received from said security processor.

13. The method of Claim 12, further directed to providing such transaction validation for different combinations of instruments and security processors without requiring changes to transaction processing by said merchant.

14. The method of Claim 12, wherein the transaction is an electronic purchase transaction.

15. The method of Claim 14, wherein the electronic purchase transaction is conducted using a digital wallet.

16. The method of Claim 12, wherein the instrument is a smart card.

17. A method for conducting a transaction, the method comprising:

a. receiving a request to authenticate a transaction at a server;

b. requiring an instrument for verification of said request;

c. receiving an instrument input response based upon said requirement;

d. processing said instrument input as an input to a security processor;

e. assembling forms for the transaction, said forms comprising said security processor authorization of said input to said security processor;

f. providing said forms for authorization;

g. processing said forms and sending a request to said security processor for a second authorization of said forms; and

h. validating said transaction with said second authorization of said forms received from said security processor.

18. The method of Claim 17, further directed to providing such transaction validation for different combinations of instruments and security processors without requiring changes to transaction processing by said merchant.

19. The method of Claim 17, wherein the transaction is an electronic purchase transaction.

20. The method of Claim 19, wherein the electronic purchase transaction is conducted using a digital wallet.

21. The method of Claim 17, wherein the instrument is a smart card.

22. A method for conducting a transaction, the method comprising:

a. receiving a request to authenticate a transaction with a merchant from a user at a server;

b. requiring the user to provide an instrument for verification;

c. receiving an instrument input response from the user based upon said requirement;

d. processing said instrument input as an input to a security processor;

e. assembling forms for the transaction, said forms comprising said security processor authorization of said input to said security processor;

f. providing said forms to said merchant;

g. said merchant processing said forms and sending a request to said security processor for a second authorization of said forms; and

h. validating said transaction with said second authorization of said forms received from said security processor.

23. The method of Claim 22, further directed to providing such transaction validation for different combinations of instruments and security processors without requiring changes to transaction processing by said merchant.

24. The method of Claim 22, wherein the transaction is an electronic purchase transaction.

25. The method of Claim 24, wherein the electronic purchase transaction is conducted using a digital wallet,

26. The method of Claim 22, wherein the instrument is a smart card.

27. A transaction system, comprising:

a. a data network, including at least one instrument and operative to permit initiation of a transaction;

b. an authorization server coupled to receive said initiation of said transaction as an input and transmit same to a security server;

c. said security server operative to receive said input from said authorization server and generate and transmit an authorization to said authorization server;

d. said authorization server coupled to receive said authorization from said security server and operative to generate and transmit an authorization form; and

e. an interface coupled to said security server and operative to permit validation of said form and complete a secure on-line virtual transaction.

28. The transaction system of Claim 27, further operative to provide said validation for different combinations of instruments and security processors.

29. The transaction system of Claim 27, wherein said authorization server is an electronic purchase server.

30. The transaction system of Claim 29, wherein said electronic purchase server is coupled to a digital wallet and operative to validate said transaction input transmitted to said security server.

31. A transaction system, comprising:

a. a data network operative to permit a user to initiate a transaction;

b. an authorization server coupled to receive an input from said user and transmit same to a security server;

c. said security server coupled to receive said input from said authorization server and operative to generate and transmit an authorization to said authorization server;

d. said authorization server coupled to receive said authorization from said security server and operative to generate and transmit an authorization form; and

e. an interface coupled to said security server and operative to permit validation of said form and complete a secure on-line virtual transaction with said user.

32. The transaction system of Claim 31, further operative to provide said form validation for different combinations of instruments and security processors.

33. The transaction system of Claim 31, wherein said authorization server is an electronic purchase server.

34. The transaction system of claim 33, wherein said electronic purchase server is coupled to a digital wallet and operative to validate said user input transmitted to said security server.

35. A transaction system, comprising:

a. a data network operative to permit initiation of a transaction with a merchant;

b. an authorization server coupled to receive said transaction initiation as an input and transmit same to a security server;

c. said security server coupled to receive said input from said authorization server and operative to generate and transmit an authorization to said authorization server;

d. said authorization server coupled to receive said authorization from said security server and operative to generate and transmit an authorization form; and

e. an interface coupled to said security server and operative to permit validation of said form and complete a secure on-line virtual transaction with said user.

36. The transaction system of Claim 35, further operative to provide said validation for different combinations of instruments and security processors.

37. The transaction system of Claim 35, wherein said authorization server is an electronic purchase server.

38. The transaction system of Claim 37, wherein said electronic purchase server is coupled to a digital wallet and operative to validate said transaction input transmitted to said security server.

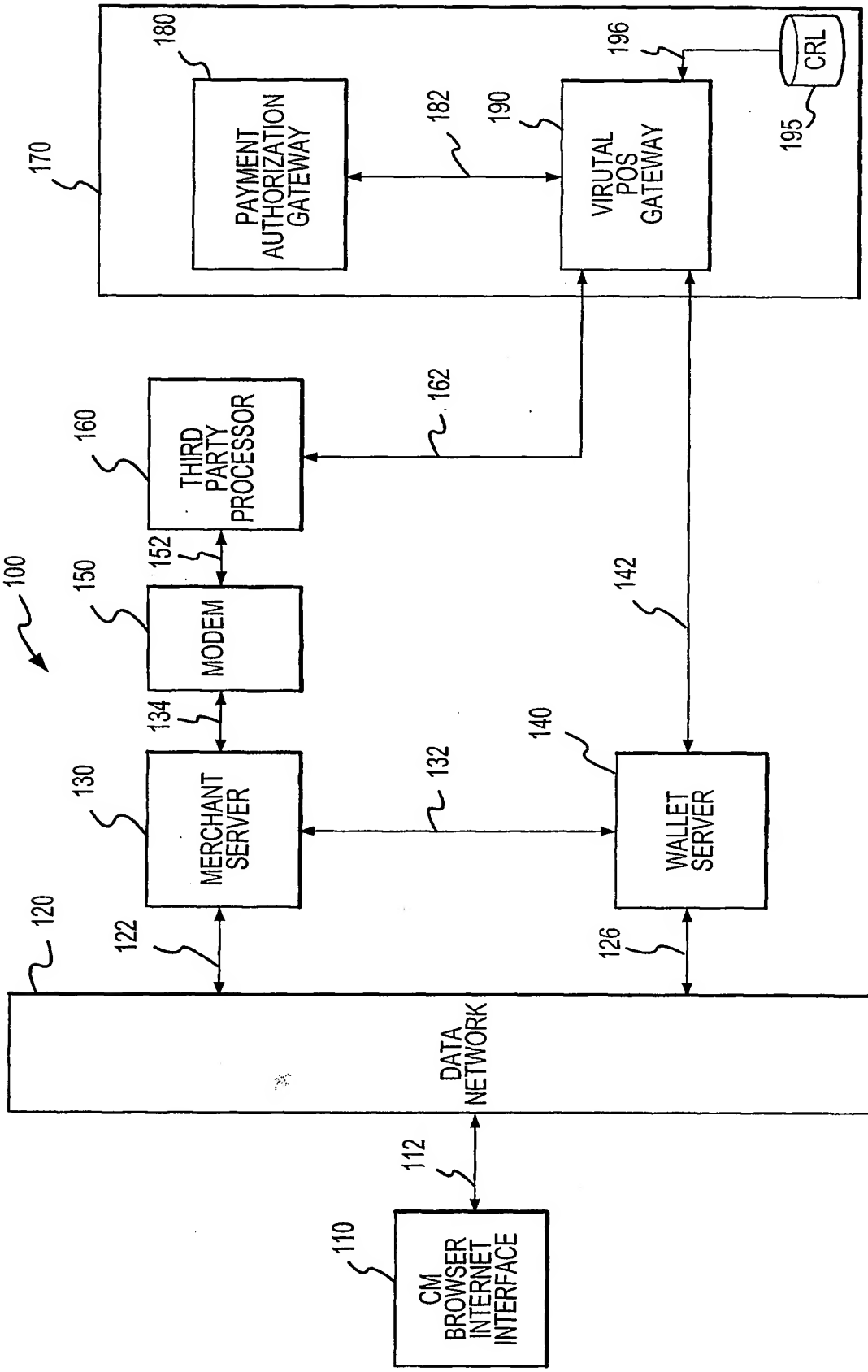


FIG.1

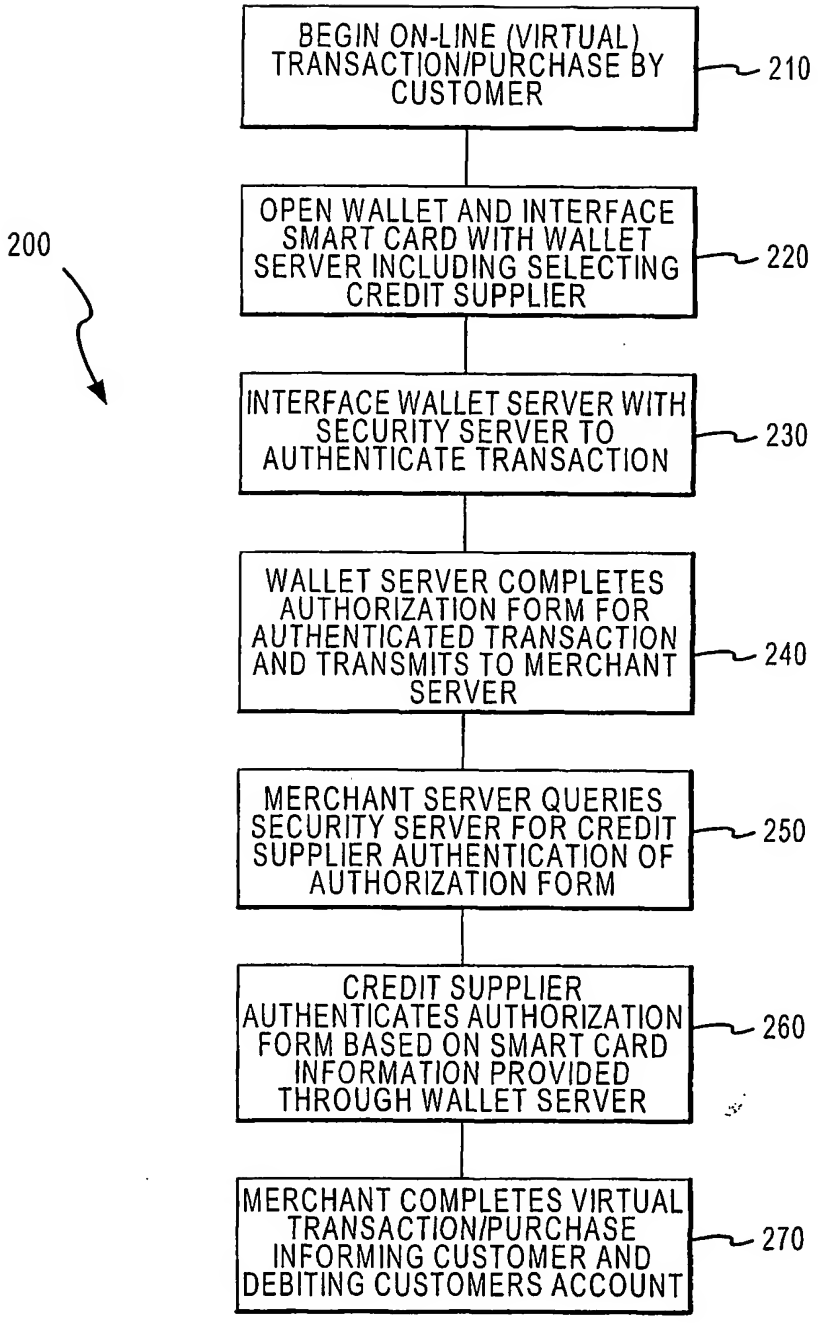


FIG.2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 01/00400

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 883 810 A (ROSEN DANIEL ET AL) 16 March 1999 (1999-03-16) abstract; claims 1,7,21; figures 1-4	1-38
Y	US 5 978 840 A (SUBRAMANIAN MAHADEVAN P ET AL) 2 November 1999 (1999-11-02) abstract; figure 10 column 14, line 35 - line 45 column 26, line 55 - line 67	1-38
E	WO 01 15034 A (DIGITALCONVERGENCE COM INC) 1 March 2001 (2001-03-01) the whole document	1-38
A	EP 0 926 637 A (NIPPON TELEGRAPH & TELEPHONE) 30 June 1999 (1999-06-30) abstract; claim 1; figure 1 column 4, line 37 -column 5, line 22	1-38

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 June 2001	13/06/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Guivol, O

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 903 721 A (SIXTUS TIMOTHY) 11 May 1999 (1999-05-11) column 6, line 33 -column 11, line 35; figures	1-38
A	EP 0 927 945 A (AMAZON COM INC) 7 July 1999 (1999-07-07) the whole document	1-38
A	US 5 500 890 A (COOPER CHRISTOPHE K ET AL) 19 March 1996 (1996-03-19) column 3, line 51 -column 4, line 16; figure 3	1,6,12, 17,22, 27,31,35
A	EP 0 813 325 A (AT & T CORP) 17 December 1997 (1997-12-17) the whole document	1,3,6, 8-12,14, 17,22, 27,31,35

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 01/00400

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5883810	A	16-03-1999	NONE		
US 5978840	A	02-11-1999	AU	4654497 A	17-04-1998
			EP	0929881 A	21-07-1999
			WO	9813797 A	02-04-1998
WO 0115034	A	01-03-2001	NONE		
EP 0926637	A	30-06-1999	JP	11265417 A	28-09-1999
US 5903721	A	11-05-1999	AU	6549498 A	29-09-1998
			DE	1008022 T	25-01-2001
			EP	1008022 A	14-06-2000
			ES	2150892 T	16-12-2000
			NO	994428 A	09-11-1999
			WO	9840809 A	17-09-1998
EP 0927945	A	07-07-1999	US	5960411 A	28-09-1999
			AU	9477998 A	29-03-1999
			CA	2246933 A	12-03-1999
			CA	2263781 A	12-03-1999
			EP	0902381 A	17-03-1999
			JP	11161717 A	18-06-1999
			JP	2000099592 A	07-04-2000
			WO	9913424 A	18-03-1999
US 5500890	A	19-03-1996	NONE		
EP 0813325	A	17-12-1997	US	5778173 A	07-07-1998
			CA	2205124 A	12-12-1997
			JP	10149397 A	02-06-1998